Билет 7

Решение квадратных уравнений в $\mathbb{Z}_p$

• $\exists p \in \mathbb{P}, p \neq 2, a, b, c \in \mathbb{Z}_p, a \neq 0, D = b^2 - 4ac$

$ax^2 + bx + c = 0 \Leftrightarrow x^2 + \frac{b}{a}x + \frac{c}{a} = 0 \Leftrightarrow$ // поделили на x

$\Leftrightarrow \left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a^2} - \frac{c}{a} =$ // перенесли

$= \frac{b^2 - 4ac}{4a^2} \Leftrightarrow \left(x + \frac{b}{2a}\right)^2 = \frac{D}{4a^2}$ // привели к одному знаменателю // расписали дискриминант!

• Если D – квадратичный вычет, то $D = d^2$ для некоторого $d \in \mathbb{Z}_p$ и $\frac{D}{4a^2} = \left(\frac{\pm d}{2a}\right)^2$ // $\pm$ – не вычет, раскрыли. Тогда уравнение имеет 2 решения:

$x_1 = \frac{-b + d}{2a}$ и $x_2 = \frac{-b - d}{2a}$ // подставили D и убрали квадрат

• Если $D = 0$, то уравнение имеет 1 решение:

$x_1 = \frac{-b}{2a}$ // потому что корень – где-то-то, когда $x = 0$

• Если D – квадратичный невычет, то $\frac{D}{4a^2}$ – также квадратичный невычет, а значит, решений нет (т.к. x^2 невычет не может быть равен квадрату по определению) // по лемме 5 о геометрических вычетах и невычетах

Билет 6

Лемма 5 $\exists p \in \mathbb{P}, a, b \in \mathbb{Z}_p, a \neq 0, b \neq 0$. Тогда:

1) Если a, b – квадратичные вычеты, то ab – квадратичный вычет.
2) Если a – кв. вычет, b – кв. невычет, то ab – кв. невычет.
3) Если a, b – кв. невычеты, то ab – кв. вычет.

D 1) $\exists$ такие $x, y \in \mathbb{Z}_p$, что $a = x^2$ и $b = y^2$. Тогда $ab = (xy)^2$. // по определению кв. вычета

2) • вычеты $a, 2a \dots (p-1)a$ (кв. вычет) – в точности все ненулевые элементы $\mathbb{Z}_p$: среди них нет 0 и все они различны, т.к. $ai = aj \Rightarrow i = j$ (равенство можно домножить на a^{-1}). (попошу что различны от 1 до $(p-1)$).

• Тогда среди этих различных элементов ровно $\frac{p-1}{2}$ квадратичных вычетов и квадратичных невычетов // по лемме 2 (лемма 4)

• Так как по п.1 при умножении a на $\frac{p-1}{2}$ кв. вычет получаем кв. вычет (различные, все $\frac{p-1}{2}$ штук), то при умножении a на $\frac{p-1}{2}$ оставшиеся элементы (невычеты) получим невычеты // так как лемма 4 выполняется! Должно быть $\frac{p-1}{2}$ (половина) вычетов по принципу остатки нужно их в невычеты

3) $a, 2a, \dots (p-1)a$ – все ненулевые элементы в $\mathbb{Z}_p$, среди них ровно $\frac{p-1}{2}$ кв. вычетов и $\frac{p-1}{2}$ невычетов. Так как при умножении a (теперь невычет!) на кв. вычеты по п. 2, получим $\frac{p-1}{2}$ кв. невычетов, то при умножении a на кв. невычет получим вычет // таким образом работает:

• тут $\frac{p-1}{2}$ вычет и $\frac{p-1}{2}$ кв. невычет

• по п.1 получили кв. вычет по определению. Их $\frac{p-1}{2}$ штук.

• Тогда при умножении вычета на невычет должны получить оставшиеся (а какие иные?!) т.е. $\frac{p-1}{2}$ невычет

• И, наконец, умножив невычет · невычет мы получаем снова половину вычетов, т.к. другая половина занята

а тут?

Вычет · вычет = вычет